PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-198955
(43)Date of publication of application : 12.07.2002

(51)Int.Cl. H04L 9/20
G06F 12/14

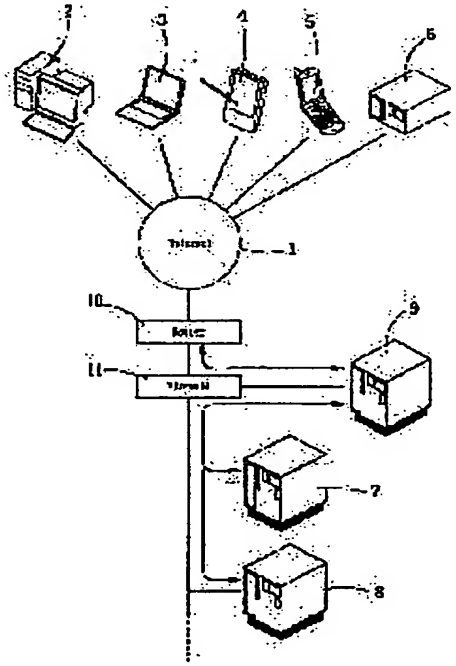
(21)Application number : 2000-398171
(22)Date of filing : 27.12.2000

(71)Applicant : FALCON SYSTEM CONSULTING KK
SHIRAI TSUTOMU

(72)Inventor : SHIRAI TSUTOMU
MIYAZAKI YUJI
IIJIMA TETSUSHI
MIZUNO TATSUO
BABA YOSHIMI

(54) WEIGHTED SECURITY SYSTEM FOR NETWORK COMMUNICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To automatically maximize communication efficiency of a network communication, and to maximize security of the network communication by using a simple system structure without reduction of the communication efficiency such as limiting the network communication as required or more and wastefully dissipating a transaction.
SOLUTION: A security system, which adds security to the network communication following a basic security system in a weighted manner, comprises a cryptographic means of data-converting transmission data, where the cryptographic means generates a key or adds the key to the transmission data.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－198955
（P2002－198955A）
(43)公開日　平成14年７月12日(2002.7.12)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　9/20		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｈ０４Ｌ　9/00	６５３	５Ｊ１０４

審査請求　未請求　請求項の数７　ＯＬ　（全８頁）

(21)出願番号　特願2000－398171(P2000－398171)

(22)出願日　平成12年12月27日(2000.12.27)

(71)出願人　300089297
ファルコンシステムコンサルティング株式会社
東京都渋谷区桜丘町29番24号　秀和桜丘レジデンス411号

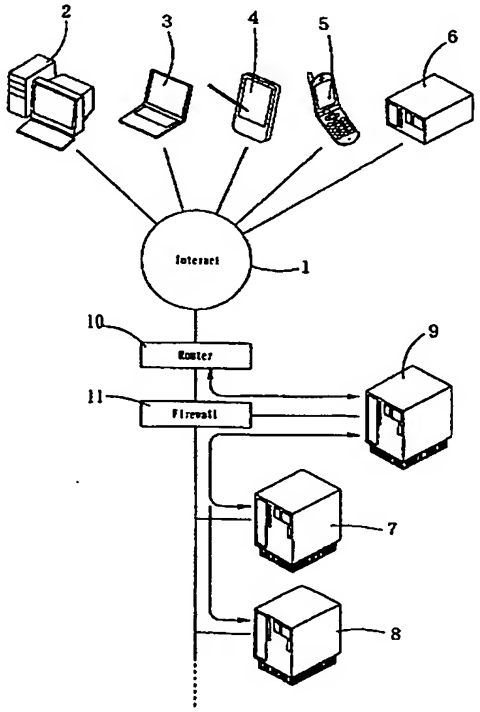
(71)出願人　500532078
白井　力
東京都渋谷区代官山町17－１　代官山アドレスタワー912号

(74)代理人　100075960
弁理士　森　廣三郎　（外１名）

最終頁に続く

(54)【発明の名称】　ネットワーク通信の加重的セキュリティシステム

(57)【要約】
【課題】　ネットワーク通信に対する通信効率を自動的に最大化し、ネットワーク通信を必要以上に制限したり、トランザクションを無駄に散逸するような効率低下を招くことなく、簡易なシステム構成で安全性の最大化を図る。
【解決手段】　基本的セキュリティシステムに従うネットワーク通信に対して加重的に付加するセキュリティシステムであって、送信データをデータ変換する暗号手段からなり、この暗号手段は前記送信データに対してリアルタイムに鍵の生成又は付加をするネットワーク通信の加重的セキュリティシステムである。



1

【特許請求の範囲】

【請求項１】　基本的セキュリティシステムに従うネットワーク通信に対して加重的に付加するセキュリティシステムであって、送信データをデータ変換する暗号手段からなり、該暗号手段は前記送信データに対してリアルタイムに鍵の生成又は付加をしてなるネットワーク通信の加重的セキュリティシステム。

【請求項２】　基本的セキュリティシステムが、TCPによるサーバからの暗号セッションからなる請求項１記載のネットワーク通信の加重的セキュリティシステム。

【請求項３】　ネットワーク通信が、クライアントが備える通信用クライアントソフトウェアに組み込まれた基本的セキュリティシステムを経て送受信されてなり、該通信用クライアントソフトウェアの基本的セキュリティシステムを通過前又は通過後の送信データに対してリアルタイムに鍵の生成又は付加をする請求項１記載のネットワーク通信の加重的セキュリティシステム。

【請求項４】　鍵が該送信データの送信毎に異なる請求項１記載のネットワーク通信の加重的セキュリティシステム。

【請求項５】　送信毎に異なる鍵が、チャレンジコードに対するレスポンスコード又はセッションキーの一方向関数値である請求項４記載のネットワーク通信の加重的セキュリティシステム。

【請求項６】　暗号手段が、携帯型プログラムである請求項１記載のネットワーク通信の加重的セキュリティシステム。

【請求項７】　クライアント側のプログラミングインターフェースを用いて、サーバからオンデマンドに暗号手段をダウンロードし、実行する請求項１記載のネットワーク通信の加重的セキュリティシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、基本的セキュリティシステムに従うネットワーク通信に対して加重的に付加するセキュリティシステムに関する。

【０００２】

【従来の技術】近年、個別に構築されたコンピュータネットワーク(以下ネットワークと略する)がインターネットに接続され、互いに見えない状況下で、多数のコンピュータ間でデータ送受信される。このようなネットワークを介したデータ送受信は、ネットワーク通信と呼ぶことができる。このネットワーク通信の安全性(完全性、機密性)を図る場合、例えばセッション確立に際してサーバとクライアントとが互いを正規と認証するため、パスワード認証を用いる。具体的には、利用者ID及びパスワードの送受信にSSLを加え、一方向認証だけではなく、(1)双方公認証(利用者側の設定が必要)及び(2)暗号化通信を図り、サーバと利用者とが互いに正規であるかどうかを確認する。RFC2828 Internet Security Glossary 等で定義されているようにSSLはSecure Socket Layerの略で、クライアントとサーバ間のトラフィックのために、データの秘匿性サービス及びデータの完備性サービスを用意する接続指向のコンピュータ間に暗号を使用するインターネットのプロトコルである。

2

【０００３】こうしたパスワード認証に対し、予めクライアントの利用者に関連する個人情報をサーバに記憶しておき、所定タイミングで個人情報及びパスワード入力をそれぞれ利用者に要求し、入力された個人情報とサーバに予め記憶した個人情報とを照合し、パスワード照合の一致及び個人情報の一致の判定を得る装置又は方法が提案されている(例えば特許第3046001号「認証装置および方法」)。サーバ及びクライアントが双方同じ利用者ID及びパスワードを用い、個人情報の一致の判定(零知識認証法)を加えてサーバがクライアントを認証するわけである。このほか、対応するチャレンジコード及びレスポンスコードの突き合せを図る認証も見られる。

【０００４】

【発明が解決しようとする課題】しかし、上記技術の零知識認証法や対応するチャレンジコード及びレスポンスコードの突き合せでは、例えばサーバから送信するチャレンジコードを読み込んだクライアント上で、その値から更に利用者が計算を積み重ねた結果としてのレスポンスコードを認証する高度な認証手法は利用されていなかった。また、通信効率最高で安全性の高い状態を維持することが可能な方式が、まだ見つかっていないという問題が存在していた。

【０００５】本発明はかかる背景に鑑み、ネットワーク通信に対する通信効率を自動的に最大化し、ネットワーク通信を必要以上に制限したり、トランザクションを無駄に散逸することなく、簡易なシステム構成で安全性の最大化を図ることを目的として、ネットワーク通信の安全性について検討した。ここで、仮に送受信データの暗号手段に問題がなくても、毎回同じ暗号手段を用いて通信すると、盗まれた送受信データから解読される問題が生じうることに着目し、ネットワークを介した認証やその後のネットワーク通信における安全性を高めることを主眼として、ネットワーク通信におけるセキュリティシステムの構築を目指した。

【０００６】

【課題を解決するための手段】検討の結果開発したものが、基本的セキュリティシステムに従うネットワーク通信に対して加重的に付加するセキュリティシステムであって、送信データをデータ変換する暗号手段からなり、この暗号手段は前記送信データに対してリアルタイムに鍵の生成又は付加をするネットワーク通信の加重的セキュリティシステムである。ここで、基本的セキュリティシステムとは、主としてTCPによるサーバからの暗号セッションからなる暗号手段、例えばSSLを例示できる。これから、本発明が対象とするネットワークは、主とし

てTCP/IPベースのネットワーク一般となり、インターネット、イントラネット、ダイアルアップ、VANサービス、エクストラネット、パソコン通信、会員制ネットワーク通信サービス、専用線等を例示できる。

【０００７】具体的には、ネットワーク通信はクライアントが備える通信用クライアントソフトウェアに組み込まれた基本的セキュリティシステムを経て送受信され、この通信用クライアントソフトウェアの基本的セキュリティシステムを通過前又は通過後の送信データに対してリアルタイムに鍵の生成又は付加をする。このとき、鍵がこの送信データの送信毎に異なるようにするとよりよい。鍵を異ならせる手法としては、(1)暗号手段そのものを変更する場合と、(2)暗号手段は同じにしながら生成又は付加する鍵そのものを変更する場合とが考えられる。また、送信毎に異なる鍵は、チャレンジコードに対するレスポンスコード又はセッションキーの一方向関数値とする、好ましくはレスポンスコード及びセッションキーを一体に一方向関数値にするとよい。

【０００８】また、暗号手段は携帯型プログラムとし、クライアント側のプログラミングインターフェースを用いてサーバからオンデマンドに暗号手段をダウンロードし、実行するシステムを構成するとよい。ここにいう「携帯型プログラム」は、主にJavaを指し、例えば暗号手段をJava Appletにより構成し、サーバからオンデマンドにクライアントへとダウンロードして実行する。クライアントとは、ネットワーク通信できる電子又は電気機器を意味し、基本的にはコンピュータを指すが、このほかPDA、Webクライアント、インターネットを利用可能な携帯電話又は専用機器等を例示できる。Javaを用いることで、クライアントにおけるハードウェアの違いを吸収でき、本発明の適用範囲を広げることができる。

【０００９】

【発明の実施の形態】以下、本発明についてまず基本概念を説明した後、具体的な例として、セッション確立に際する認証と、認証に続くネットワーク通信(より具体的にはデータ送信)について説明する。図１は本発明を適用する一般的なネットワーク形態におけるハード構成図、図２は本発明を用いたサーバとクライアントとのやりとりを表した全体フローチャート図、図３はセッション確立に際する認証をモデルとした本発明のネットワーク通信を説明するデータ送受信相関図で、図４はクライアントにおけるデータ送受信の流れを表した論理説明図である。各例は、最も簡易な例として基本的セキュリティシステムにSSLを利用しているが、SSLに代えて別のセキュリティシステムを用いてもよい。基本的セキュリティシステムの種類を問わないのは、本発明が基本的セキュリティシステムに対して付加的に用いる加重的セキュリティシステムだからであり、本発明の汎用性を示す特徴である。

【００１０】本例は、インターネット１を介して、利用者がクライアント２，３，４，５(デスクトップ型コンピュータ２、ノート型コンピュータ３、PDA又はWebパッド４、インターネット利用可能な携帯電話５や専用機器６等、以下クライアント２で代表)に搭載するブラウザ(通信用クライアントソフトウェア)を用いてサービス提供サーバ７に接続する例で、クライアント２は認証サーバ９を介してサービス提供サーバ７にアクセスする。認証サーバ９は、認証データベース８から利用者情報を参照して、認証にかかる処理を実行する。ここで、本例に示すサービス提供サーバ７は、Webサーバ、mailサーバ又はFTPサーバ等を指し、単一のハードである必要はなく、提供するサービス内容によって、各種データベースや他システムと組み合わせて構成する。

【００１１】本発明を適用するハード構成図は、図１に見られるように、インターネット１を介したサーバ(認証サーバ９、サービス提供サーバ７)とクライアント２とを接続する。クライアント２は、インターネット１を介してルータ10に至り、ファイアウォール11を経て認証サーバ９に接続し、認証データベース８を参照した認証サーバ９による接続認証及び利用認証を受けた後、サービス提供サーバ７にアクセスできる(図２参照)。本例では、アクセス間隔に時間制限(Time Out値の設定)を設け、認証後一定時間(Time Out値)内に利用がない場合に再認証を要することとして、安全性を高めている。

【００１２】本発明を適用したサーバ及びクライアント間では、図３及び図４に見られるように、まずブラウザを用いてSSLによる基本的なセッションを確立し、ユーザーID等を用いたパスワード認証を経て、チャレンジコード及びレスポンスコードの突き合せにより高い安全性を確保したセッションを確立する。これらのセッションに必要なプログラムは、最初のクライアントからサーバに向けてのSSLセッション確立を除いて、サーバからクライアントへダウンロードする携帯型プログラム(Java Applet)に従う。そして、認証後は、再びサーバからクライアントへ鍵生成のための携帯型プログラム(Java Applet)をダウンロードし、クライアントは前記携帯型プログラムに従ってデータ送信することになる。

【００１３】次に、セッション確立に際する認証を具体的に説明する。図５は本発明の(1)基本システムを用いた接続認証及び利用認証の部分フローチャート図である。利用者は、クライアント２に搭載したブラウザを用いてSSLによる認証サーバ９(図１参照、以下同じ)へのアクセスを図る。本発明は、ブラウザが有するSSLのサーバ認証手段(基本設定機能として予め設定され、特に新たな設定を要しない)を基本的セキュリティ手段に付加して用い、利用者の利便性を高めると共にデータ送受信に関わる通信上の安全性(完全性、機密性)を高めている。本例のサーバ認証はこのSSLに基づき、図５に見られるように、利用者認証は従来公知の利用者ID及びパスワードに基づく接続認証と、サービス提供サーバ７利用

に際する基本システムを用いた利用認証とを用いる。

【００１４】まず、クライアント２で認証サーバ９にアクセスを開始すると、処理手順送信プログラムが識別コード(利用者ID(及びパスワード))入力要求プログラム及び識別コード返信プログラムをクライアント２へ送信し、利用者に利用者ID(及びパスワード)を求める。利用者は、識別コード入力要求プログラムに従って利用者ID及びパスワードを入力すると、続いて識別コード返信プログラムが前記利用者ID(及びパスワード)を認証サーバ９に返信する。そして、認証サーバ９が利用者ID(及びパスワード)を確認すると、利用者認証(接続認証)される。例えば、クライアント２がサーバ管理者から貸与された専用機器６である場合、各専用機器６に固有利用者ID等を内蔵させておき、自動的に固有利用者IDを認証するようにしておけば、接続認証にかかる利用者の手続は省略可能である。

【００１５】接続認証を終えると、続く利用認証のためのアクセスがクライアント２に許される。まず、認証サーバ９は利用者情報を認証データベース８から検索し、利用者毎に登録したチャレンジコード群を取得し、前記チャレンジコード群からランダムに１つのチャレンジコードを選択する。前記一連の処理は、(a)コード選択手段を構成するコード選択プログラムに基づく。コード選択プログラムの実行は認証サーバ９上であるため、プログラム言語の種類は問わない。チャレンジコードは、予めサーバに登録された複数のチャレンジコード及びレスポンスコードの組から選択する。

【００１６】次に、(b)データ送信手段を構成するデータ送信プログラムにより、特定したチャレンジコード、(C)入力要求手段を構成する入力要求プログラム、(d)受信コード作成手段を構成する受信コード作成プログラム、(e)データ返信手段を構成するデータ返信プログラム、変換手段を構成するデータ変換プログラム、現在アクセスを試みている利用者のカウンタ(アクセス累積数)とタイムスタンプ(アクセス開始時間)とをクライアント２へ送信する。これらの送信にはSSLを利用し、送信上の完全性、機密性を確保している。データ変換プログラムは受信コード作成プログラムと一体でもよい。いずれのプログラムも、クライアント２の機種の違いに依存しないJava(Java Applet)で形成する。携帯電話５等、一度に多くのJavaを受信できないものは、各プログラムを順次送信してもよい。この場合、前の処理プログラムに、処理終了を通知する機能を付加しておく。

【００１７】(C)入力要求プログラム、(d)受信コード作成プログラム、(e)データ返信プログラム、データ変換プログラム、カウンタ及びタイムスタンプを受信したクライアント２は、まず(c)入力要求プログラムに従って、クライアント２の画面上にチャレンジコードを表示又は発声し、対応するレスポンスコードの入力を促す。このレスポンスコードの入力は、通常キーボードを用いた文字入力であるが、音声入力による声紋認証(携帯電話５等)、手書き文字入力による筆跡認証(PDA又はWebパッド４等)、個人の身体的特徴を利用するバイオメトリックス認証、ICカード等を利用した保有者認証等を、個別又は組み合わせて利用できる。

【００１８】利用者によりレスポンスコードが入力されると、(d)受信コード作成プログラムが、前記レスポンスコードとカウンタ及びタイムスタンプとを一体にデータ変換プログラムによりデータ変換して受信コード(鍵)を作成する。この認証における「鍵」は、あくまでセッション確立のためのものである。本例では、データ変換プログラムとしてHASH関数(一方向関数)を用い、MDからなる受信コード(鍵)を作成する。カウンタやタイムスタンプはアクセスの度に数値が異なるセッションキー(経時的変数)であり、例えば前回同様のレスポンスコードからでも送信毎に異なる受信コードを作ることができる。これにより、返信段階で受信コードが盗まれても、次回のアクセスにおける認証の真正性が保証できる。また、受信コードは認証を図る双方のみが知る正しいHASH関数でなければ確認が取れないため、完全性が高い。本例では、更に受信コードをSSLで返信することで安全性を高めている。

【００１９】こうして得られた受信コード(鍵)は、(e)データ返信プログラムによってクライアント２から自動的に返信され、認証サーバ９が受信する。認証のみを目的とした場合、(C)入力要求プログラム、(d)受信コード作成プログラム、(e)データ返信プログラム、データ変換プログラム、カウンタ及びタイムスタンプは、受信コード返信後消滅することが望ましい。こうした消滅処理を担うプログラムは、(e)データ返信プログラムに含め、受信コード返信後自動的に実行させるとよい。このように、本発明の認証システムでは、クライアント２に認証のための特別なプログラムを搭載しなくてもよい利点がある。本例では、受信コードの返信にSSLを利用している。

【００２０】クライアント２より受信コードを受信した認証サーバ９は、(f)認証コード作成手段を構成する認証コード作成プログラムにより、先に(b)データ送信プログラムによりクライアント２へ送信したチャレンジコードに対応するレスポンスコードと同じくクライアント２へ送信したカウンタ及びタイムスタンプとを一体に、同じくクライアント２へ送信したデータ変換プログラムを用いてデータ変換、すなわち認証コード(鍵)を作成する。このデータ変換処理は認証サーバ９上で実施するため、プログラム言語は問わないが、データ変換アルゴリズム自体はクライアント２へ送信したデータ変換プログラムと一致しておく必要がある。これから分かるように、どのようなデータ変換プログラムを用いるかは認証サーバに決定権があり、例えばクライアント２が同じでもアクセス毎にデータ変換プログラムを変更することも

できる(後述図７参照)。

【００２１】認証サーバ９及びクライアント２が共に正規であれば、クライアント２から返信されてきた受信コード(鍵)と、認証サーバ９が作成した認証コード(鍵)とは一致する(完全性がある)。(g)相手方認証手段を構成する相手方認証プログラムは前記完全性判断を担う。利用者が正規であれば、認証サーバ９が示したチャレンジコードに正しく対応したレスポンスコードにより受信コードが構成されており、当然に認証コードと完全一致するはずである。これにより、認証サーバ９はクライアント２を正規利用者利用のクライアントと認証できる。こうして、接続認証、利用認証が正規に終了すれば、認証サーバ９は自身を介したクライアント２のサービス提供サーバ７へのアクセスを許可する(図２参照)。

【００２２】図６は(2)拡張システムを用いた接続認証及び利用認証の部分フローチャート図である。基本的な処理の流れは基本システムと変わりはないが、複数のレスポンスコードとカウンタ及びタイムスタンプとを一体にデータ変換した１つの受信コード(鍵)は、前記レスポンスコードがすべて正しくないと、認証コード(鍵)と一致しない(完全性がない)ことになり、安全性が高められる。また、(a)コード選択手段が選択する複数のチャレンジコードは、必ずしも一定数でなくてもよく、安全性向上のために選択個数ｎを変更することが可能である。選択個数ｎをランダムにするには、例えば乱数を用いる。

【００２３】図７は(2)拡張システムに対して(3)応用システムを用いた接続認証及び利用認証の部分フローチャート図である。予め認証サーバ９に複数のデータ変換プログラム(同種又は異種データ変換プログラムを複数)を搭載しており、(a)コード選択プログラムが予め登録されているチャレンジコード群の中から複数のチャレンジコードを選択するのと同様に、(a')変換選択プログラムが予め登録されているデータ変換プログラム群の中から１つのデータ変換プログラムを選択する。

【００２４】(3)応用システムにおいて、アクセスの度にデータ変換プログラムの変更可能なのは、本システムが認証サーバ９に必要な処理プログラムをすべて有し、利用者認証に際して認証サーバ９からクライアント２へ送信するからである。これにより、認証サーバ９において、データ変換プログラム群を適宜更新又は変更して、常に最新のデータ変換プログラムを用いた高い機密性を得ることができる。従来一般に見られるようにクライアント２にも同種のデータ変換プログラムを要するとすれば、認証サーバ９及びクライアント２双方がデータ変換プログラムを一致させておかなければならず、適宜更新又は変更が難しい。このように、本発明はデータ変換プログラムの管理又はメンテナンスの観点からも好ましいシステムとなっている。

【００２５】本発明は、上述のように認証に際して安全なセッションの確立を図ることができるほか、そのままネットワーク通信の基本セキュリティ手段(上記ではSSL)に付加してデータ送受信の加重的な安全性確保に利用できる。つまり、繰り返されるネットワーク通信における過去の送信データから推測される攻撃を防ぐため、送信データに対して生成又は付加する鍵を送信毎に異ならせるわけである。上記例に即して説明すれば、認証後のデータ送受信(実際にはデータ送信)において、サーバからクライアントへ送信した(d)受信コード作成プログラム、(e)データ返信プログラム、データ変換プログラム、カウンタ及びタイムスタンプを利用する。具体的には、クライアントからサーバへの送信データに対し、(d)受信コード作成プログラムにより(1)レスポンスコード、(2)カウンタ又は(3)タイムスタンプを個別又は選択的に選んでデータ変換プログラムに従ってデータ変換し、鍵を生成する。すなわち、データ送信に際しては、(d)受信コード作成プログラムが鍵生成プログラムとなる。こうして生成した鍵を用いて更に暗号化した送信データを(e)データ返信プログラムがサーバへと送信する。

【００２６】「鍵を用いて更に暗号化した送信データ」は、単にデータを暗号化するのみならず、既述した認証同様の突き合わせる鍵として機能したり、データの改竄確認の役割も果たす。暗号化した送信データは、通信時における改竄確認を図るほか、サーバに保管しておくことで、事後に改竄の有無を確認できるようにするわけである。従来も同様な役割を果たす鍵(例えば公開鍵方式による暗号化)も存在するが、これらは鍵の生成又は暗号化のためのプログラムをクライアントが持っている必要があり、プログラムの管理又はメンテナンスが難しい問題を有している。これに対し、本発明はサーバがすべての手段を有しているので、前記問題が存在しない利点がある。

【００２７】ここで、送信毎に(1)新たなデータ変換プログラムを用いたり、(2)カウンタ又は(3)タイムスタンプを更新して鍵を生成すると、送信毎に用いる鍵を異ならせることができ、ネットワーク通信における安全性をより高めることができる。また、決済情報等のように、毎回類似の内容を有するデータを送信する場合、各データの略同位置に類似のデータが並ぶことになりやすいが、例えば(d)受信コード作成プログラムにおいてデータの並びを変更する機能(一種の暗号化)を付加し、生成した鍵により前記変更後のデータを暗号化するとよい。こうしたデータの取扱いについての柔軟性は、各プログラムはすべてサーバが有しており、必要に応じて仕様や内容を適宜変更してクライアントへダウンロードできる運用の柔軟性に基づく効果と言える。

【００２８】

【発明の効果】本発明により、ネットワーク通信における送信データの完全性(盗用者による割込みや送受信デ

ータの置換の防止)、機密性(盗用者のよる送受信データの解析防止)を高め、安全性の高いセキュリティシステムを提供できるようになる。特徴として、完全性及び機密性確保に必要な各手段をすべてサーバが有するので、クライアントになんら搭載せずにシステム構成を一括又は部分的(特にデータ変換手段)に更新可能な点を挙げることができる。これは、従来のセキュリティシステムが更新を含むシステム管理にあった不便さを解消する利点である。

【００２９】一方向関数を用いた処理は高速で通信効率の低下を招かず、機密性が高い点も利点である。また、レスポンスコードはデータ変換するため、コードのそのものが通信路上に現れることがなく、機密性が高い。更に、受信コードは経時的に変化するセッションキーを加えてデータ変換しているために経時的特異性を有し、更に通信上の機密性を高めている。こうして、本発明は正規利用者のみが正しいサーバとセッションを確立し、完全性及び機密性を保ってデータ送信できるというネットワーク上の信頼性を実現する。

【００３０】上記例示では、サーバに対してクライアントを接続する場合を示したが、本発明はサーバを媒介としてクライアント相互を接続する場合や、このクライアント相互のデータ送信にも利用可能である。サーバを媒介とするクライアント相互では、サーバが本発明に必要な各手段を搭載し、各利用者が正規であることの確認を図る態様となる。すなわち、利用者は各手段を必要とせず、各利用者は適宜異なるクライアントを用いて接続及びデータ送信が可能となる。

【図面の簡単な説明】

【図１】本発明を適用する一般的なネットワーク形態におけるハード構成図である。

【図２】サーバと利用者とのやりとりを表した全体フローチャート図である。

【図３】セッション確立に際する認証をモデルとした本発明のネットワーク通信を説明するデータ送受信相関図である。

【図４】クライアントにおけるデータ送受信の流れを表した論理説明図である。

【図５】(1)基本システムを用いた接続認証及び利用認証の部分フローチャート図である。

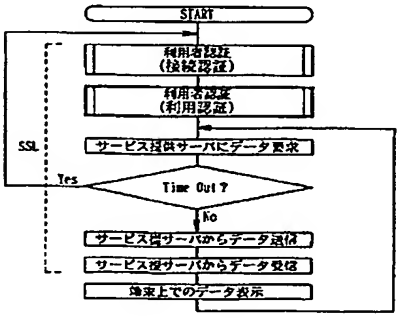
【図６】(2)拡張システムを用いた接続認証及び利用認証の部分フローチャート図である。

【図７】(3)拡張システムに対して応用システムを用いた接続認証及び利用認証の部分フローチャート図である。

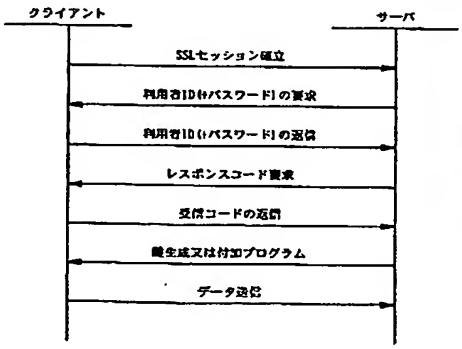
【符号の説明】

1　インターネット
2　デスクトップ型コンピュータ
3　ノート型コンピュータ
4　PDA又はWebパッド
5　インターネット利用可能な携帯電話
6　専用機器
7　サービス提供サーバ
8　認証データベース
9　認証サーバ
10　ルータ
11　ファイアウォール

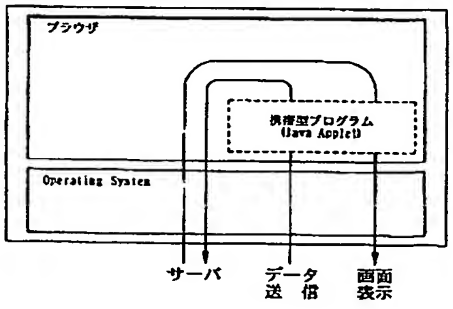
【図２】



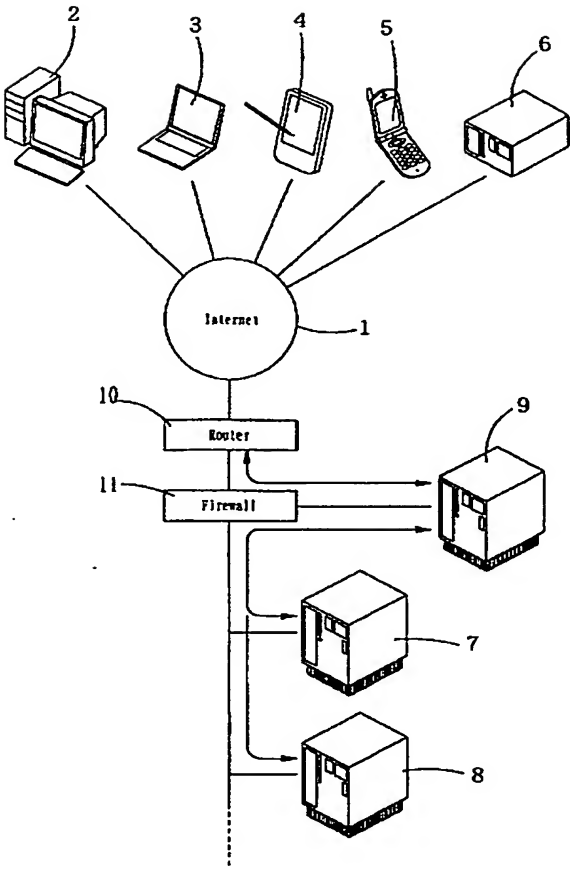
【図３】



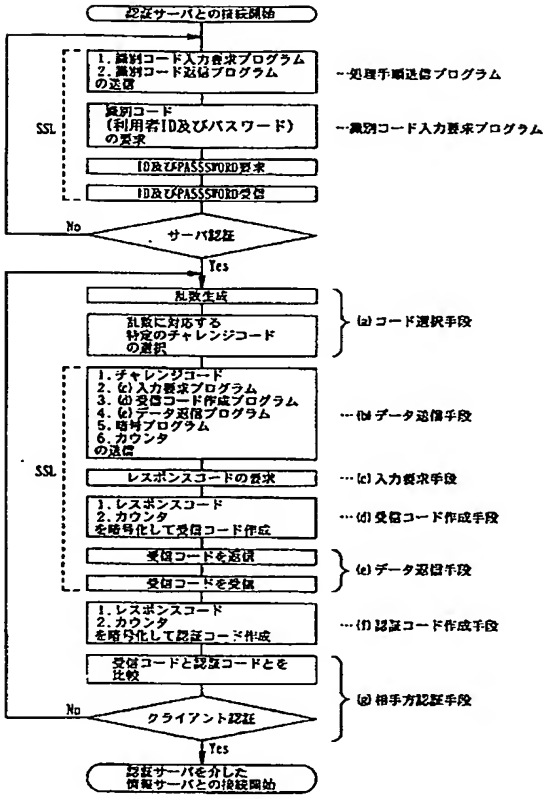
【図４】



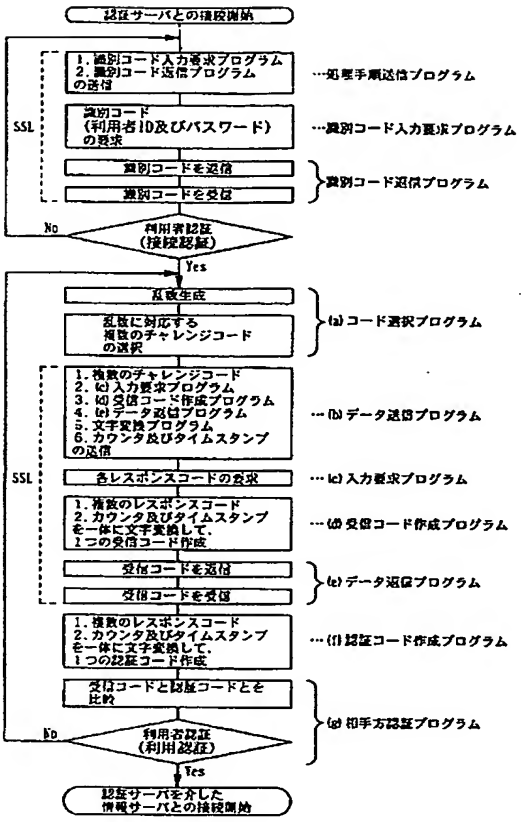
【図１】


2
3
4
5
6
Internet
1
10
Router
11
Firewall
9
7
8

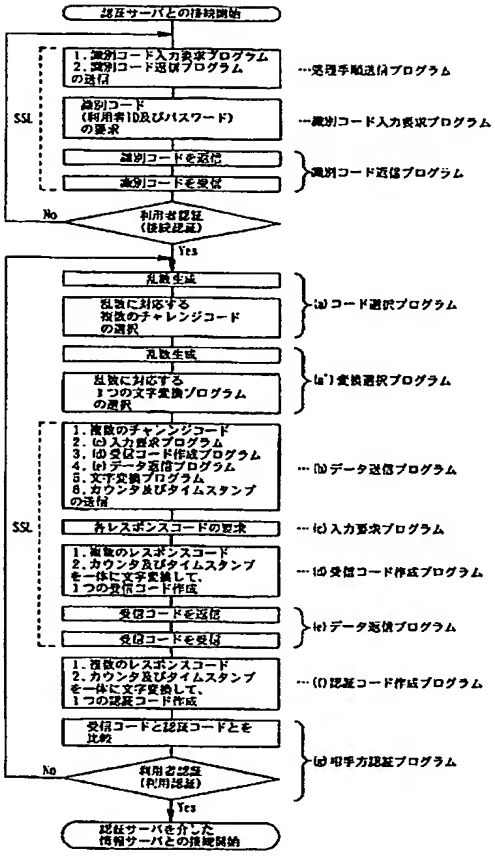
【図５】


認証サーバとの接続開始
1. 識別コード入力要求プログラム
2. 識別コード送信プログラム
の送信
…処理手順送信プログラム
SSL
識別コード
(利用者ID及びパスワード)
の要求
…識別コード入力要求プログラム
ID及びPASSSWORD要求
ID及びPASSSWORD受信
No
サーバ認証
Yes
乱数生成
乱数に対応する
特定のチャレンジコード
の選択
(a) コード選択手段
1. チャレンジコード
2. (c) 入力要求プログラム
3. (d) 受信コード作成プログラム
4. (e) データ送信プログラム
5. 暗号プログラム
6. カウンタ
の送信
…(b) データ送信手段
SSL
レスポンスコードの要求
…(c) 入力要求手段
1. レスポンスコード
2. カウンタ
を暗号化して受信コード作成
…(d) 受信コード作成手段
受信コードを送信
受信コードを受信
(e) データ送信手段
1. レスポンスコード
2. カウンタ
を暗号化して認証コード作成
…(f) 認証コード作成手段
受信コードと認証コードとを
比較
No
クライアント認証
(g) 相手方認証手段
Yes
認証サーバを介した
情報サーバとの接続開始

【図６】



【図７】



フロントページの続き

(72)発明者　白井　力
東京都渋谷区代官山町17－１　代官山アドレスタワー912号
(72)発明者　宮崎　裕司
東京都狛江市和泉本町１－６－10　パークスクエア狛江103
(72)発明者　飯嶋　鉄志
東京都八王子市暁町２－17－６
(72)発明者　水野　健生
神奈川県横浜市神奈川区三ツ沢南町４－５
(72)発明者　馬場　芳美
神奈川県横浜市港北区太尾町644

Ｆターム(参考)　5B017 AA03 BA07 BB09
5J104 AA07 AA11 AA16 AA41 EA04
EA16 KA01 KA06 KA09 KA21
NA03 NA05 NA11 NA12 PA07